

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 08-314805
(43)Date of publication of application : 29.11.1996

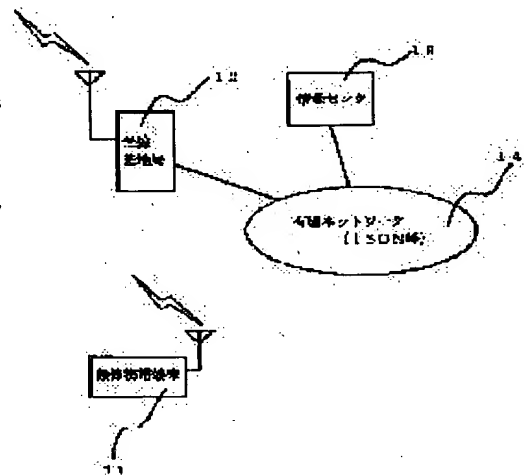
(51)Int.Cl. G06F 12/14
G06F 15/00

(21)Application number : 07-121853 (71)Applicant : NEC CORP
(22)Date of filing : 19.05.1995 (72)Inventor : ARIGA KENICHI

(54) SYSTEM FOR PREVENTING PORTABLE RADIO TERMINAL FROM BEING ILLEGALLY USED AND METHOD FOR EXECUTING THE SAME

(57)Abstract:

PURPOSE: To prevent a portable radio terminal from being illegally used by providing a means for erasing internal data after the completion of backup copy.
CONSTITUTION: A portable radio terminal 11 judges the illegal use of the terminal and transmits an illegal use report message to an information center 13. At the information center 13, a system data dump request message is transmitted for the backup copy of internal data in the portable radio terminal 11. On the side of the portable radio terminal, the transmission of internal data is started after the system data dump request message was transmitted. These system data of the portable radio terminal 11 are sent every packet as unit and at the information center 13, a reception confirm message is transmitted to the portable radio terminal 11 for every packet. After the completion of backup copy, the information center 13 transmits a system lock request message to the portable radio terminal 11. At the portable radio terminal 11, a system lock complete message is transmitted, the internal data are erased, and the portable radio terminal 11 is turned to be in an unusable state and locked.



LEGAL STATUS

[Date of request for examination] 19.05.1995
[Date of sending the examiner's decision of rejection] 30.04.1997
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19) 日本国特許庁(JP)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平 8 - 3 1 4 8 0 5

(43) 公開日 平成8年(1996)11月29日

(51) Int. Cl. ⁶	識別記号	庁内整理番号	F I	技術表示箇所
G 0 6 F	12/14	3 2 0	G 0 6 F	12/14 3 2 0 D
	15/00	3 3 0		15/00 3 3 0 C

審査請求 有 請求項の数 7 O L (全 5 頁)

(21) 出願番号 特願平7-121853

(22) 出願日 平成7年(1995)5月19日

(71) 出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(72) 発明者 有賀 健一

東京都港区芝五丁目7番1号 日本電気株式会社内

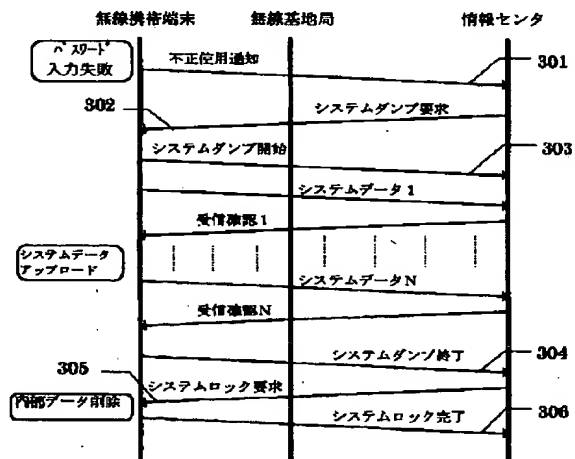
(74) 代理人 弁理士 鈴木 弘男

(54) 【発明の名称】 無線携帯端末不正使用防止システム及びその実施方法

(57) 【要約】

【目的】 本発明の目的は、紛失したか、または盗難された無線携帯端末が所有者以外の者によって力を不正使用されることを防止して、セキュリティの向上を図ることにある。

【構成】 本発明は、無線携帯端末を操作開始するためのパスワードを規定回数失敗すると、無線携帯端末を管理している情報センタに不正使用されている旨を自動的に通知し、それを受けて無線携帯端末は内部データを暗号化して情報センタにダンプを行い、情報センタにおけるバックアップコピーのとり終りに無線携帯端末の内部データをすべて削除するように構成されている。



【特許請求の範囲】

【請求項 1】 情報センタに登録されてそのサービスを受けている無線携帯端末の不正使用防止システムであって、

前記無線携帯端末に設けられた、パスワード入力を行うための入力手段と、

該パスワード入力が所定回数誤って行われたことを前記情報センタに通知するように無線携帯端末に設けられた送信手段と、

前記情報センタからの指示に基づいて、前記無線携帯端末の内部データのバックアップコピーを前記情報センタ内の記憶装置にとる手段と、

該バックアップコピーのとり終りに該内部データを消去する手段と、を具備することを特徴とする無線携帯端末不正使用防止システム。

【請求項 2】 情報センタに登録されてそのサービスを受けている無線携帯端末の不正使用防止システムであって、

前記無線携帯端末に設けられた、パスワード入力を行うための入力手段と、

該パスワード入力が所定回数誤って行われたことを検出するように前記情報センタに設けられた検出手段と、

前記情報センタからの指示に基づいて、前記無線携帯端末の内部データのバックアップコピーを前記情報センタ内の記憶装置にとる手段と、

該バックアップコピーのとり終りに該内部データを消去する手段と、を具備することを特徴とする無線携帯端末不正使用防止システム。

【請求項 3】 情報センタに登録されてそのサービスを受けている無線携帯端末の不正使用防止方法であって、前記無線携帯端末の入力手段を介してパスワード入力を行うことと、

該パスワード入力が所定回数誤って行われたことを前記情報センタに通知することと、

前記情報センタからの指示に基づいて、前記無線携帯端末の内部データのバックアップコピーを前記情報センタ内の記憶装置にとることと、

該バックアップコピーのとり終りに該内部データを消去すること、の各ステップからなることを特徴とする無線携帯端末不正使用防止方法。

【請求項 4】 情報センタに登録されてそのサービスを受けている無線携帯端末の不正使用防止方法であって、前記無線携帯端末の入力手段を介してパスワード入力を行うことと、

該パスワード入力が所定回数誤って行われたことを情報センタにおいて検出することと、

前記情報センタからの指示に基づいて、前記無線携帯端末の内部データのバックアップコピーを前記情報センタ内の記憶装置にとることと、

該バックアップコピーのとり終りに該内部データを消

去すること、の各ステップからなることを特徴とする無線携帯端末不正使用防止方法。

【請求項 5】 前記バックアップコピーをとる際に、前記情報センタから前記無線携帯端末に送信されるシステムデータダンプ要求メッセージが前記無線携帯端末のシステムデータを暗号化するためのキーデータを含むことを特徴とする請求項 3 および請求項 4 のいずれかに記載の無線携帯端末不正使用防止方法。

【請求項 6】 前記無線携帯端末の内部データが前記情報センタから送られてくる暗号キーを用いて暗号化されることを特徴とする請求項 3 および請求項 4 のいずれかに記載の無線携帯端末不正使用防止方法。

【請求項 7】 前記無線携帯端末のシステムデータがパケット単位で送られると共に、前記情報センタにおいてはパケット毎に受信確認メッセージが送信されることを特徴とする請求項 5 に記載の無線携帯端末不正使用防止方法。

【発明の詳細な説明】

【0001】

【産業上の利用分野】 本発明は無線携帯端末における不正使用に対するネットワークを介した防止システムとその実施方法に関する。

【0002】

【従来の技術】 近年、無線携帯端末が世の中に普及しつつあるが、無線携帯端末のセキュリティ確保についてはまだまだ発展途上段階にある。従来の無線携帯端末の中には紛失したり盗難にあつたりした場合のセキュリティを確保するために、パスワードを設定しそれを起動時に入力させるようになっているものがある（例えば、特開昭 63-10260 号公報参照）。また、IC カードに個人のパスワードを記憶しておき、その IC カードを端末に入れることによってホストに接続するようなものがある（例えば、特開平 2-226456 号公報参照）。

【0003】 特開平 2-226456 号公報には、ユーザが入力する第 1 の識別コードと、このユーザが利用するカードに記録されている第 2 の識別コードとの対が、ホストに設けられている識別コードテーブルと一致したときのみ使用可能にする計算機システムについて記載されている。

【0004】

一方、特開平 2-112053 号公報には、外部から供給されるパスワードと内部に保有するパスワードとの一致／不一致を判定し、判定結果が一致する場合に内部に保有するパスワードを所定の規則に従って更新することにより、セキュリティの向上を図るデータ処理方法について記載されている。

【0005】

【発明が解決しようとする課題】 無線携帯端末を紛失または盗難され、その端末を第三者が取得して不正に使用することを試みた場合、パスワード機能がなければ自由に無線ネットワークへのアクセスや住所録などの内部デ

ータの参照が可能である。またパスワード機能があっても、無制限にパスワード入力を繰り返すことが可能ならば、何らかの手段によってパスワードを解読され、不正使用を防止することはできない。

【0006】

【発明の目的】本発明の目的は、盗難に遭ったか、または紛失した無線携帯端末が所有者以外の者によって不正使用されることを防止して、セキュリティの向上を図るようにした無線携帯端末不正使用防止システムおよびその実施方法を提供することである。

【0007】

【課題を解決するための手段】上記目的を達成するために、本発明の第1態様によれば、情報センタに登録されてそのサービスを受けている無線携帯端末の不正使用防止システムであって、前記無線携帯端末に設けられた、パスワード入力を行うための入力手段と、該パスワード入力が所定回数誤って行われたことを前記情報センタに通知するように無線携帯端末に設けられた送信手段と、前記情報センタからの指示に基づいて、前記無線携帯端末の内部データのバックアップコピーを前記情報センタ内の記憶装置にとる手段と、該バックアップコピーのとり終りに該内部データを消去する手段とを具備することを特徴とする無線携帯端末不正使用防止システムが提供される。

【0008】本発明の第2態様によれば、情報センタに登録されてそのサービスを受けている無線携帯端末の不正使用防止システムであって、前記無線携帯端末に設けられた、パスワード入力を行うための入力手段と、該パスワード入力が所定回数誤って行われたことを検出するように前記情報センタに設けられた検出手段と、前記情報センタからの指示に基づいて、前記無線携帯端末の内部データのバックアップコピーを前記情報センタ内の記憶装置にとる手段と、該バックアップコピーのとり終りに該内部データを消去する手段とを具備することを特徴とする無線携帯端末不正使用防止システムが提供される。

【0009】本発明の第3態様によれば、情報センタに登録されてそのサービスを受けている無線携帯端末の不正使用防止方法であって、前記無線携帯端末の入力手段を介してパスワード入力を行うことと、該パスワード入力が所定回数誤って行われたことを前記情報センタに通知することと、前記情報センタからの指示に基づいて、前記無線携帯端末の内部データのバックアップコピーを前記情報センタ内の記憶装置にとることと、該バックアップコピーのとり終りに該内部データを消去することの各ステップからなることを特徴とする無線携帯端末不正使用防止方法が提供される。

【0010】本発明の第4態様によれば、情報センタに登録されてそのサービスを受けている無線携帯端末の不正使用防止方法であって、前記無線携帯端末の入力手段

を介してパスワード入力を行うことと、該パスワード入力が所定回数誤って行われたことを情報センタにおいて検出することと、前記情報センタからの指示に基づいて、前記無線携帯端末の内部データのバックアップコピーを前記情報センタ内の記憶装置にとることと、該バックアップコピーのとり終りに該内部データを消去することの各ステップからなることを特徴とする無線携帯端末不正使用防止方法が提供される。

【0011】以上4個の基本態様に加えて、本発明は次のような実施態様を有する。まず、上記第3および第4態様のいずれかに記載の無線携帯端末不正使用防止方法において、バックアップコピーをとる際に、情報センタから無線携帯端末に送信されるシステムデータダンプ要求メッセージが無線携帯端末のシステムデータを暗号化するためのキーデータを含む。

【0012】また、上記第3および第4態様のいずれかに記載の無線携帯端末不正使用防止方法において、無線携帯端末の内部データが情報センタから送られてくる暗号キーを用いて暗号化される。

【0013】さらに、無線携帯端末のシステムデータはパケット単位で送られると共に、前記情報センタにおいてはパケット毎に受信確認メッセージが送信される。

【0014】

【作用】所有者以外の第三者が無線携帯端末を使用してこの無線携帯端末を使用するためのパスワードを予め決められた回数以上謝ると、無線携帯端末は情報センタに対して不正使用の通知を行ない、この通知により情報センタは端末内部のデータバックアップをとった後に端末の内部データを消去する要求を無線携帯端末に送信し、無線携帯端末を使用不可の状態にする。これによって盗難された無線携帯端末の不正使用を防止することができる。

【0015】

【実施例】以下、本発明を添付の図面に示す好ましい実施例に関連してさらに詳細に説明する。図1は本発明に用いられる無線携帯端末システムの全体構成図であり、図2は本発明に用いられる無線携帯端末のハードウェア構成を示すブロック図であり、図3は本発明の第1実施例の動作を示すシーケンス図であり、図4は本発明の第2実施例の動作を示すシーケンス図である。

【0016】まず、図2を参照して本発明に用いられる無線携帯端末のハードウェア構成が説明される。

【0017】無線携帯端末は、システム全体を制御するCPU21、制御プログラム等が蓄積されているROM24、制御プログラムが使用するワーク用RAM22、住所録やスケジュールなどの個人データが蓄積されているデータ蓄積用RAM23、情報や操作を表示するための表示器25、データを入力するための入力装置26、無線の制御を行なう無線モジュール27で構成されている。

5

【0018】入力装置26で入力されたデータはデータ蓄積用RAM23に蓄積される。

【0019】一般的にデータ蓄積用RAM23は電池でバックアップされているために、電源を落としても消去されることはない。無線でデータの送信を行なう場合には、RAM22、23、ROM24からシステムバスを通じて、無線モジュール27にデータが送られ、これによってデータの送信が行われる。

【0020】次に無線携帯端末システムの全体構成を図1を用いて説明する。

【0021】いま、所有者以外の第三者が不正使用をしようとしている無線携帯端末を11とする。無線携帯端末11は情報センタ13に登録、管理されていて、有線ネットワーク14に接続されている情報センタ13に対して無線基地局19を通じてアクセスできるようになっている。

【0022】図3のシーケンス図を用いて本発明の第1実施例の動作を説明する。

【0023】今、所有者以外の第三者が無線携帯端末11を不正に用いようとして、パスワード入力を試み、システムで規定されている回数の入力誤りを起こしたとする。この時、無線携帯端末11は、端末が不正使用されようとしていると判断して、これを情報センタ13に通知するために不正使用通知メッセージを情報センタ13に送信する。【301】

不正使用通知メッセージを受信した情報センタ13では、無線携帯端末11の内部データのバックアップコピーをとるためにシステムデータダンプ要求メッセージを送信する。【302】

このメッセージには無線携帯端末11のシステムデータを暗号化するためのキーデータを付加する。無線携帯端末側でこのメッセージを受信すると、システムデータダンプ開始メッセージを送信した後、内部データの送信を開始する。【303】

内部データは無線を通じて不正に取り込まれないように、情報センタ13から送られてきた暗号キーを用いて、暗号化される。

【0024】無線携帯端末11のシステムデータはパケット単位で送られ、情報センタ13ではパケット毎に受信確認メッセージを無線携帯端末11に送信する。【304】

情報センタ13は、バックアップコピーのとり終り後に、システムロック要求メッセージを無線携帯端末11に送信する。無線携帯端末11ではこのメッセージを受信後にシステムロック完了メッセージを送信して、内部

6

データを消去して無線携帯端末を使用不可の状態にしてロックする。【305-306】

本発明の第2実施例として、システムで規定された回数だけパスワードの入力誤りを起こしたことを情報センタで検出する場合の動作が図4のシーケンス図に示される。この第2実施例では、無線携帯端末11の不正使用が情報センタ13において判断されるので、前述の第1実施例における無線携帯端末11から情報センタ13への不正使用通知メッセージの送信動作は不要になる。それ以外は第1実施例と同じ動作が行われるので、重複を避けるためにそれらの説明を省略する。

【0025】

【発明の効果】以上説明したように、本発明の無線携帯端末不正使用防止方法は、第三者によって取得された無線携帯端末を不正に用いようとして、誤ったパスワード入力を数回試みると無線携帯端末内部のデータが消去して端末をロック状態にするために、無線携帯端末を紛失したり盗難にあたりした後に、第三者が無線ネットワークへのアクセスや住所録などの内部データを参照することができなくなり、無線携帯端末のセキュリティが保たれる。また内部データを消去する前にデータのバックアップコピーを管理先の情報センタに備えられた記憶装置にとって置くので、正規の持ち主によってなされる再使用時における復旧が容易である。

【図面の簡単な説明】

【図1】本発明で用いられる無線携帯端末システムの全体構成図である。

【図2】本発明で用いられる無線携帯端末のハードウェア構成を示すブロック図である。

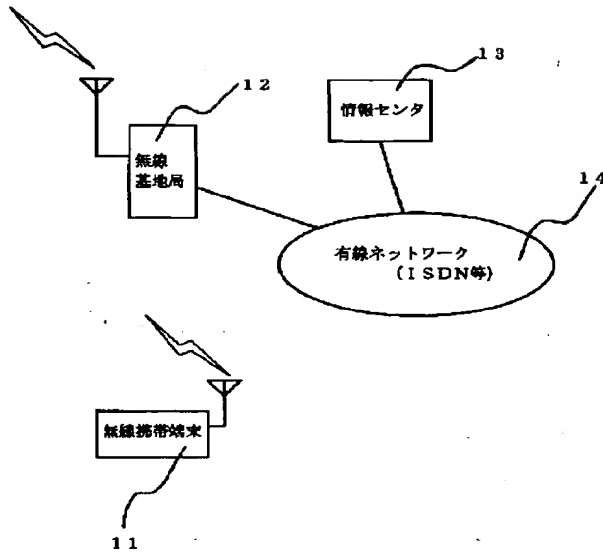
【図3】本発明の第1実施例の動作を示すシーケンス図である。

【図4】本発明の第2実施例の動作を示すシーケンス図である。

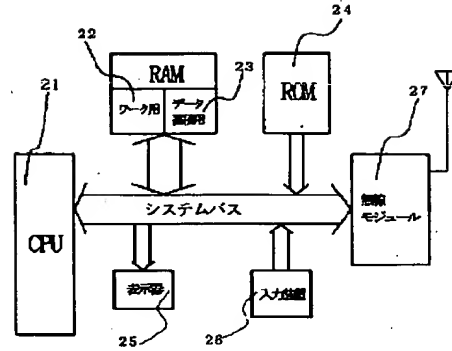
【符号の説明】

- 11 無線携帯端末
- 12 無線基地局
- 13 情報センタ
- 14 有線ネットワーク
- 21 CPU
- 22 ワーク用RAM
- 23 データ蓄積用RAM
- 24 ROM
- 25 表示器
- 26 入力装置
- 27 無線モジュール

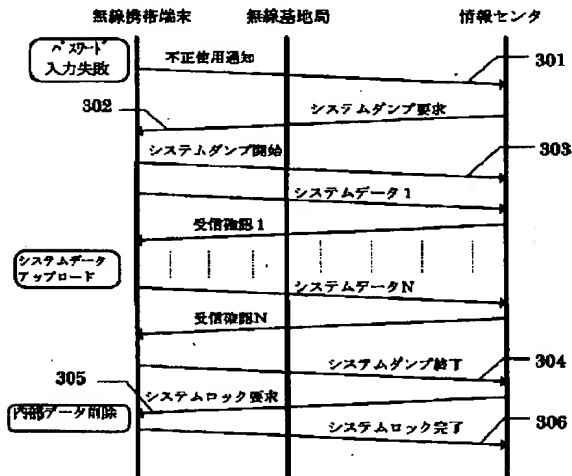
【図1】



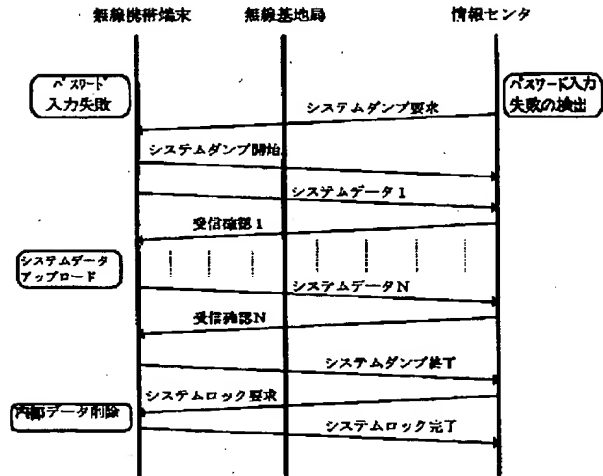
【図2】



【図3】



【図4】



**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☐ **FADED TEXT OR DRAWING**
- ☒ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☐ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:** _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.